MARCH 2018
IMPORTANT DAYS

4th • The Oscars (90th Academy Awards)
8th • International Women's Day
9th-18th • 2018 Winter Paralympics
11th • Daylight Savings Time
17th • St. Patrick's Day
30th • Good Friday

Aveir

Tech Times

5 Ways To Prepare For, Respond To, And Recover From A Cyberattack

When we asked businesses about cybersecurity threats, breach points, policies, company readiness, and recovery, we were surprised at the responses that we received. The most frightening response of all was the following: *"We have no formal process for assessing readiness to deal with a cyberattack of any sort."* Hindsight is always 20/20 – how many times has something happened that you could have and should have prevented? Here are five ways to prepare every company for a cyberattack:

Cybersecurity Threats
It's easy to sit back and think that threats and attacks only happen to other people and other businesses, but not to ourselves. Living in a state of paranoia can be beneficial to the security of your company. Former Intel CEO, Andrew Grove, once stated that "Only the paranoid survive." Knowing all you can about current and possible future attacks helps you to understand why and how you need to be prepared.

Cyberattack Sources Of Breaches
Cyberattacks could threaten your business through a few different sources. For example, employee mobile devices make up for 51% of all cybersecurity breaches, which is extremely troubling, given that there are nearly as many employee cell phones as there are employees themselves. Another possible source of a breach is Internet of Things devices. Together they make up 87% of all the cybersecurity breaches.

Cybersecurity Policies
Cybersecurity policies should be in place to ensure that the company as a whole is all in agreement on what the threats are, how to avoid them, and how to respond to one. Employees should be trained to know how to report a possible cyberattack, as well as how to prevent one.

Cybersecurity Attack Readiness
To check your business for its readiness to handle a cyberattack you should see which of the four main categories your company falls into. Is your organization's readiness passive, reactive, proactive, or progressive? Passive means that your business is not prepared for a cyberattack – you just hope that it won't happen. Reactive means that while you aren't ready to protect against a cyberattack, your business is prepared to react to one.

Recovery From Cyberattacks
Once a cyberattack has occurred, you need to have a policy in place to immediately begin recovery. Cyberattacks have four main effects. In the aftermath, most businesses will see a reduction in their operational abilities, downtime, reputation, and revenue.

To protect your business, you need to look at the problem from all sides. Ensure that you and your staff are well trained, and remain vigilant against any cyberattack that could affect your company. Have policies in place, to ensure that staff is proactively working to protect the business' data, staff, and clients. Should a cyberattack occur, your business should be ready to not only combat it but also recover from it?

Will 2018 Bring The Rise Or Fall Of Cybersecurity?

A relatively new set of guidelines enacted in the European Union requires many global organizations to reconsider their security practices and update their protective measures.

A quick review of 2017 suggests that it was the worst year on record for cybersecurity – phrases like "data breach", "phishing", and "hackers" were uttered in the news so often that we numbed to the shock factor. Checking our credit reports and changing our passwords yet again for banking, credit cards, email, and everything else that impacts daily life is now nearly a quarterly requirement.

What makes cybersecurity such a complex concept is that it's something we can't see and that most consumers can't even fully understand. These are the very elements that put consumers at the greatest risk because fighting an enemy when we don't know its weaknesses seems challenging, but when the enemy knows ours, it's terrifying. Cybercriminals are always working to stay one step ahead of the latest steps that consumers take to protect themselves.

What can we expect in 2018? It's safe to assume that things may get worse before they get better. In many ways, organizations are still playing catch-up when it comes to cybersecurity. Hackers continue to outthink the latest developments in cybersecurity – and how? Because we make it too easy.

Yes, we make it easy – a breakdown in the corporate communication chain, not enough allocations in the budget, and inefficiencies in our security personnel or protocol are just a few of the factors that contribute to why we can't keep up with hackers.

Is tech about to become all doom and gloom? Not a chance – and those fighting back are doing so with a vengeance. It's true that governing bodies can't pass legislation fast enough to keep up with hackers, but it's also true that we can't expect hackers to fear the law or those who enforce it.

Have you heard of the General Data Protection Regulation (GDPR)? In early 2016, the European Parliament began mandating that companies who operate in, do business with, or ultimately collect data on citizens in EU countries will be subject to strict rules enacted to protect these consumers.

Knowing the dangers of misaddressed e-mails is only half the battle. What can we do to prevent it and protect the integrity of our business?

Consider the last time you received an email from a friend or colleague that seemed like their email address was compromised. It was likely a message promoting hair growth vitamins, or from someone claiming to be from Google who recommended you reset your password immediately – but neither the web link nor the "from" email address had anything to do with Google. These seemed like obvious threats that are easy enough to ignore.

What happens if a hacker gains access to the webcam on your laptop and read your personal data through the reflection in your eyeglasses? This seemed far-fetched a decade ago, but today? It's a genuine concern. Imagine that type of scenario but a hundredfold in complexity, and with access to global consumer data – what do you need to do to be ready?

Knowledge is power: arm yourself with an arsenal of information and be transparent in all professional relationships. We'll face 2018 together, and emerge stronger in 2019 – together.

Shocking Fact Revealed: 53% Of Businesses Are Publicly Exposed

How Businesses Are Accidentally Exposing Cloud Services – Don't Make The Same Mistakes

Malware comes in many different forms and is used by hackers in a number of different ways. It can be used to steal information, locate vulnerabilities in your IT systems for a secondary attack, or simply to cause damage.

There are countless hackers out there just waiting for your business to leave your data vulnerable. With the introduction of the cloud, you felt a bit more secure and slept slightly better at night – but now, it seems that was precisely what hackers wanted us to do.

It's reported that 53% of businesses using cloud storage accidentally expose their data to the public. This is like securing your whole house, locking all doors and windows, and then going to sleep with the garage wide open.

This doesn't just point the finger at small businesses either. The study showed that even big-name companies such as Amazon Simple Storage Service (Amazon S3) had inadvertently exposed one or more of these services to the public. The scary thing is that the previous survey showed this was occurring only 40% of the time. Now, this number has grown to 53%.

This study was conducted in 2017 between the months of June to September. Within those two months, they found that businesses are not only exposing their own data but they are also neglecting vulnerabilities in their cloud. When you ignore these things, you put not only your customers at risk but also the livelihood of your company as well.

What Are You Exposing?

The report shows that businesses weren't solely leaking data such as customer information, but incredibly dangerous information such as access keys and other private data as well. These cyber-attacks commonly expose data such as personal health information, financial information, passwords and usernames, trade secrets, and intellectual property. With two million new malware attacks launching every day, it's more important than ever to stay in a constant state of vigilance.

Ignoring Vulnerabilities

A common misconception is that it's the service provider's responsibility to keep cloud data safe – this is not true. Most of the damage caused by ignoring vulnerabilities can be prevented by training. If your staff is trained to recognize weaknesses, then they can be more proactive in fighting against them. More than 80% of businesses are not managing host vulnerabilities in the cloud. Vulnerabilities include insufficient or suspicious credentials, application weaknesses, and inadequate employee security training.

Complex Attacks

Not all the attacks and vulnerabilities are the fault of the business. Some of these attacks are far more complex than most businesses are prepared for, including big-name companies. These sophisticated attacks not only know and bypass the company's vulnerabilities but also various application weaknesses.

What Can You Do About It?

The first action you can take against attacks like this is recognizing suspicious IP addresses. Have a policy in place for identifying, flagging, and isolating suspicious IP addresses. Spending a few extra minutes of your time could save months of recovery and downtime.

It's important to pay attention to mistakes that others have made so that you don't suffer the same consequences. Be sure to train and certify the IT staff you already have – cyberattacks are all but guaranteed. What isn't guaranteed is how prepared your business is to thwart off those attacks.

Tech Tip of the Month:

7 Surprising Ways To Prepare Your Website For Cyberattacks

Keep hackers from turning you and your business into a victim with these cybersecurity best practices.

Cyberattacks come in many forms, and no part of your business seems to be safe from them. You work for months to prepare your website. You go into painstaking detail over each section and prepare for your go-live date. You are so proud to show your corporate baby to the world. Then a few months later, you go to log into your website to find it has been hacked. Not only does this affect your business data and reputation, but also your position in Search engines. How do you keep this hypothetical from becoming your reality?

Stay Up-to-date With Cyberattack News
The best offense is a good defense. To prepare for, respond to, and recover from an attack, you need to know what you are up against. You can prepare for Cyberattack by keeping up to date on current cyber threats to your company. Over 2 million new malware attacks are launched every day, with recent examples including the Meltdown and Spectre bugs. Both Spectre and Meltdown could allow potential attackers to access to data, but these aren't your only threats. You need to also prepare for other Cyberattacks such as Ransomware, crypto, and malware attacks. Forbes magazine reports these are the top cybersecurity threats to look out for in 2018.

Update Security On Your Login Page
Similarly to your email password, you should take great care in protecting your website admin access. You should use strong passwords so they can't be easily guessed or forged. Secondly, you should memorize your website passwords, rather than write them down, as this poses another security risk. Thirdly, remember to change the password frequently – it is recommended that you do so every two months.

Update Software
Updates always seem to come when we are at our busiest. Whenever there's an opportunity to update, it's essential to do so. Updating is like having a secret security group continually working to keep your business safe. Updates provide protective patches that safeguard your data from the latest cyberattacks, such as Meltdown or Spectre. Plus, they keep your computers and systems running optimally.

Security Plugins
Security plugins offer your website features that range from protection against malware attacks to an added firewall and database security. Each plugin comes with own cost and features – for example, one of the highest-ranking WordPress plugins is WordFence. This plugin continually scans your folders and files on your website for signs of malware infection. Once it finds an infection, it can rapidly notify you as it blocks the malware. Another WordPress plugin that packs a lot of features into a small package is Sucuri Security. Through this plugin, you can have security activity auditing, file integrity monitoring, malware scanning, blacklist monitoring, as well as a website firewall.

HTTPS Instead Of HTTP
How much difference can one letter make? Between an HTTPS and HTTP, surprisingly it makes a massive difference for security. Hyper Text Transfer Protocol Secure is the version of HTTP which transfers data from your browser and your website. The difference is that one letter "S" – secure. This means that any and all communication between your browser and your site is protected with encryption.

Secure Web Hosting
Another way to strengthen the security of your website is by using a secure web hosting company. There are lots of big and small names to choose from when deciding on a web hosting provider. This is where it is essential to use your list of non-negotiable features that you want from your host to narrow down your choices. For example, you could look for a host that offers a Virtual Private Server, which conceals the identity of your service and improves privacy. Another important feature to look for when deciding is how many users it can support.

Lock Files/Folders
One of the simplest ways to improve the security of your website is by locking or hiding files. You can place passwords on files or folder, that way they cannot be opened without your key. Additionally, you can also encrypt them so that they are unreadable without your password. You can do this by using a password-protection system or using file permissions that are already in place. Check to see what features your web host offers.

With all the ways that a hacker can gain access to your business's data, it is crucial to stay one step ahead. Remember the importance of securing your website as well. Something as simple as a secure password for your admin page or locking specific files can make a huge difference for you and your business.

February Special

Run Your Staff Thru Our Spring Training Cybersecurity Awareness Lunch

Book For Free Today.

Call 775.329.2400 or email sales@aveir.com to reserve your free cybersecurity lunch training with our security specialists.

Hurry, offer good through March 31.

Quotes of the Month

"It's the fans that need spring training. You gotta get 'em interested. Wake 'em up and let 'em know that their season is coming, the good times are gonna roll."
Harry Caray

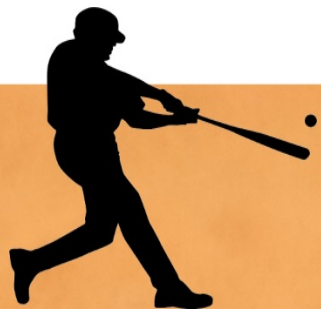
"I've always approached spring training as I have something to prove."
Jamie Moyer

"I come to spring training and just try to do my job, try to do the best I can. That's all any player can do."
Danny Bautista

Funny Business

Aveir

Aveir Technology
1400 S. Virginia St.
Suite B
Reno, NV 89502
775.329.2400
www.aveir.com



Run Your Staff Thru Our Spring Training Cybersecurity Awareness Lunch. Book for Free Today.

Call 775.329.2400 or email sales@aveir.com to reserve your FREE cybersecurity lunch training with our security specialists. Hurry, offer good through Mar. 31.